UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,538	06/21/2005	Claudia Becker	P0837US00/RFH	1217

881 7590 04/02/2009

STITES & HARBISON PLLC
1199 NORTH FAIRFAX STREET
SUITE 900
ALEXANDRIA, VA 22314

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,538	BECKER ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 09/03/2004. Claims 1-16 are pending and have been considered as follows.

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-4, 6, 7, 11-14, & 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1 lines 15-35 recite "the true value" and "the restored control word" and "the latter" which lack antecedent basis.
- Claim 2 lines 25-28 recite "for which the status variable is that of said status variable" which is indefinite as it appears to recite itself;
- Claim 3:
    - Line 2 recites "proper" which is unclear;
    - Line 3 recites "the latter" which lacks antecedent basis;
    - Line 5 recites "in verifying the existence" which is unclear given the rest of the language;
    - Lines 9-16 recite "on a positive response to said verification" and "on a positive response to said posterity nature verification" however, the placement of these limitations which appear to support the start of a new limitation makes it awkward and difficult to understand and follow; that is, perhaps each new bullet "-" should start with their above respective opening condition(s) instead of the current layout;

- Claim 4:
    - Line 4 recites "the latter" which lacks antecedent basis;
    - Lines 4-5 recite "in addition in performing" which is unclear and reads awkwardly;
- Claim 6 lines 2-4 recite "proper" and "the latter" where "proper" is unclear and "the latter" lacks antecedent basis;
- Claim 7 lines 20-23 recite "the latter" which lacks antecedent basis;
- Claim 11 line 4 recites "the latter" which lacks antecedent basis;
- Claim 12 line 4 recites "the latter" which lacks antecedent basis;
- Claim 13 line 4 recites "the latter" which lacks antecedent basis;
- Claim 14:
    - Lines 3-6 recites "this access control module" which lacks antecedent basis; for the purposes of examination it appears this limitation is referring to the "module controlling access";
    - Lines 19-21 recite "can have" which is indefinite as to whether it "can" "have";
- Claim 16:
    - Lines 4-6 recite "said access rights" which is unclear as to which "access right";
    - Lines 4-6 recite "said access rights defining" which lacks antecedent basis;
    - Lines 7-8 recite "the subscribing user" which lacks antecedent basis;
    - Lines 7-8 recite "the holder" which lacks antecedent basis;

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 & 14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 1:
  - recites "a protocol" which appears to be comprised of nothing more than computer software/program modules, which is non-statutory subject matter;
  - "a protocol" is also not one of the statutory categories for patentability;
  - note that the preamble of Claim 1 appears to be non-functional descriptive material or functional but merely descriptive material, thus has not been given patentable weight at this point in time
  - (the examiner recommends the incorporation of structural limitations that would clearly claim the use of technology which permits the function of the non-functional/functional descriptive material to be realized);
- Claim 14:
  - recites "a module" which appears to be comprised of nothing more than computer software/program modules, which is non-statutory subject matter;
  - "a module" is also not one of the statutory categories for patentability;
  - note that the preamble of Claim 1 appears to be non-functional descriptive material or functional but merely descriptive material, thus has not been given patentable weight at this point in time

- (the examiner recommends the incorporation of structural limitations that would clearly claim the use of technology which permits the function of the non-functional/functional descriptive material to be realized);

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore (US-6697489-B1).

Claim 1:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is

provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20] comprising,

- "transmitting from said transmission center to each descrambling terminal and to the access control module linked to the latter at least one access right management message, said message comprising at least, in addition to an entered access right identification variable, an action date variable and a status assignment variable, the encoded value corresponding to an enabled access right, a disabled access right or an erased access right; and on receipt of said access right management message, at said access control module" (i.e. "These copy management commands may also be transmitted along with entitlement control messages (ECM), which are generally used by the conditional access unit to regulate access to a particular channel or service. Entitlement management messages (EMM) may be used to deliver privileges to the digital receiver 111 such as rights, access parameters, and descrambling keys") [column 3 line 67 & column 4 lines 1-6];

- "allocating said status assignment variable corresponding to an enabled access right, a disabled access right or an erased access right to said status variable of said corresponding entered access right" (i.e. "The access requirements and entitlements thus form a part of the access control system to determine whether a decoder is authorized to view a particular program") [column 4 lines 62-65];

but, Candelore does not explicitly disclose,

- "forming any access right entered in said access control module as a set of independent variables and linked variables comprising at least, in addition to an access right identification variable, an entered access right action date variable and a status variable which can have one of three encoded values signifying access right enabled, access right disabled, access right erased," although Candelore does suggest entitlements, as recited below;
- "assigning said action date to the entered access right corresponding to the access right identification variable of said access right management message," although Candelore does suggest a validity time, as recited below;

however, Candelore does disclose,

- "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65];
- "the Service Key may be valid for a certain period of time" [column 8 lines 66-67];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "assigning said action date to the entered access right corresponding to the access right identification variable of said access right management message," in the invention as disclosed by Candelore for the purposes of providing access control for subscriber content.

Claim 2:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 1 above, further comprising,

- "for an operation to enter a defined access right in an access control module, said action date variable of said access right management message corresponds to an entry date, and the status assignment variable is an encoded value corresponding to an enabled right, the entry operation consisting in entering, into said access control module, a defined access right, the action date of which is that of said entry date and for which the status variable is that of said status variable and corresponds to an enabled right" (i.e. "the Service Key may be valid for a certain period of time" [column 8 lines 66-67].

Claim 3:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the

descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 2 above, further comprising,

- "prior to the entry operation proper of said defined access right, the latter consists in addition, in said access control module, in verifying the existence, in said access control module, of an entered access right corresponding to said defined access right and for which the status variable corresponds to the encoded value signifying right enabled or right disabled" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65];
- "on a positive response to said verification: in verifying the posteriority nature of said action date variable corresponding to an entry date in relation to the action date of said identical access right" (i.e. "the Service Key may be valid for a certain period of time" [column 8 lines 66-67];
- "on a positive response to said posteriority nature verification, performing an update of said action date variable of said identical access right, based on said action date corresponding to an entry date" (i.e. "the Service Key may be valid for a certain period of time" [column 8 lines 66-67];
- "assigning, to said status variable of said identical access right, the encoded value corresponding to an enabled right, allowing said entered access right to be enabled" (i.e. "the access requirements for the program are compared to the entitlements that the

conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 4:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 2 above, further comprising,

- "on a negative response to said verification of the existence of an identical access right, the latter consists in addition in performing an update by first entry of this access right, for which the action date corresponds to the entry date" (i.e. "the Service Key may be valid for a certain period of time" [column 8 lines 66-67].

Claim 5:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 1 above, further comprising,

- "for an operation to disable an access right entered in an access control module, said action date variable of said access right management message corresponds to a disabling date and the status assignment variable is an encoded value corresponding to a disabled right, the disabling operation consisting in assigning, to said status variable of said entered access right, said encoded value corresponding to a disabled right and updating said action date of said entered access right based on said disabling date" (i.e. "the Service Key may be valid for a certain period of time. The decoder 701 may store the key as it surfs to other services, allowing the decoder to re-access the service with a still valid key without having to request the key again" [column 8 lines 66-67].

Claim 6:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler

integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 1 above, further comprising,

- "prior to the disabling operation proper, the latter consists in: verifying the existence, on said access control module, of an entered access right corresponding to said access right of said management message" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65];
- "verifying the posteriority nature of said action date variable corresponding to a disabling date with respect to said action date variable of said entered right" (i.e. "the Service Key may be valid for a certain period of time. The decoder 701 may store the key as it surfs to other services, allowing the decoder to re-access the service with a still valid key without having to request the key again" [column 8 lines 66-67].

Claim 7:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control

word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 1 above, further comprising,

- "for any status assignment variable of the management message corresponding to an erased access right and for any access right entered in the access control module for which the status variable corresponds to an enabled right or a disabled right, the latter consists at least in: an update of the action date of said entered right" (i.e. "the Service Key may be valid for a certain period of time. The decoder 701 may store the key as it surfs to other services, allowing the decoder to re-access the service with a still valid key without having to request the key again" [column 8 lines 66-67];
- "an allocation, to said status variable of said entered access right, of said status assignment variable of the management message corresponding to an erased access right, said allocation operation forming, for said entered access right, a virtual erasure operation" (i.e. "the access requirements for the program are compared to the

entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 8:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 7 above, further comprising,

- "the update and virtual erasure steps of said entered access right are preceded by a step to verify the existence, on said access control module, of an entered access right corresponding to said access right of said management message, and a step to verify the posteriority of said action date variable of said management message with respect to said action date variable of said entered access right" (i.e. "the Service Key may be valid for a certain period of time. The decoder 701 may store the key as it surfs to other services, allowing the decoder to re-access the service with a still valid key without having to request the key again" [column 8 lines 66-67].

Claim 9:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of

the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 7 above, further comprising,

- "said virtual erasure operation is followed by a physical erasure operation of said access right" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 10:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler

integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 9 above, further comprising,

- "said physical erasure operation is immediate or deferred" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 11:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated

circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 2 above, further comprising,

- "for an entered access right for which the status assignment variable corresponds to an erased access right, the latter also consists in performing an update by first entry of this access right, said access right being assigned a status variable corresponding to an enabled right and for which the action date corresponds to the entry date" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 12:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against

said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 5 above, further comprising,

- "for an entered access right for which the status assignment variable corresponds to an erased access right, the latter also consists in performing an update by first entry of this access right, said access right being assigned a status variable corresponding to a disabled right and for which the action date corresponds to the entry date" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 13:

Candelore discloses a protocol for entering, disabling/erasing scrambled data access rights transmitted from a transmission center to at least one descrambling terminal to which is linked an access control module equipped with a security processor, these access rights being entered in

said access control module, said scrambled data being subjected to an access control by periodic transmission of access control messages, conveying access criteria and a cryptogram of a control word that is changed periodically and encrypted using an operation key, then, in each security processor, conditionally upon verifying the true value of at least one entered access right against said access criteria, by decrypting the cryptogram of the control word using said operation key, transmitting the restored control word to the descrambling terminal and descrambling said scrambled data using said restored control word (i.e. "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word") [column 3 lines 10-20], as in Claim 5 above, further comprising,

- "on a negative response to said verification of the existence of a corresponding access right, the latter also consists in performing an update by first entry of this access right, for which the action date corresponds to a disabling date, said access right being assigned a status variable corresponding to a disabled right" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional access unit is entitled to view content…entitlements may also include one or more keys…entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Claim 14:

Candelore discloses a module controlling access to scrambled data transmitted from a transmission center to at least one descrambling terminal to which is linked this access control module, but, Candelore does not explicitly disclose,

- "characterized in that it comprises, entered in the memory of this access control module, at least one access right formed by a set of independent variables and of linked variables, comprising at least, in addition to an entered access right identification variable and a validity dates variable, an entered access right action date variable and a status variable that can have one of three encoded values signifying access right enabled, access right disabled or access right erased" although Candelore does suggest a method for securing control words, as recited below;

however, Candelore does disclose,

- "a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word" [column 3 lines 10-20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "characterized in that it comprises, entered in the memory of this access control module, at least one access right formed by a set of independent variables and of linked variables, comprising at least, in addition to an entered access right identification

variable and a validity dates variable, an entered access right action date variable and a status variable that can have one of three encoded values signifying access right enabled, access right disabled or access right erased," in the invention as disclosed by Candelore for the purposes of providing access control for subscriber content.

Claim 15:

Candelore discloses a module controlling access to scrambled data transmitted from a transmission center to at least one descrambling terminal to which is linked this access control module, as in Claim 14 above, further comprising,

- "since said access control module comprises a microprocessor card fitted with a security processor and a secured non-volatile programmable memory, said at least one access right is entered in said secured non-volatile programmable memory" [FIG 7 illustrates a processor with memory used in access control of encrypted content & control words].

Claim 16:

Candelore discloses a module controlling access to scrambled data transmitted from a transmission center to at least one descrambling terminal to which is linked this access control module, as in Claim 14 above, further comprising,

- "for an access control to scrambled data for a pay television service, said access rights cover said access rights defining the modes of access to said scrambled data and electronic purses allocated to the subscribing user, the holder of said access control module" (i.e. "the access requirements for the program are compared to the entitlements that the conditional access unit actually has…entitlements may state that the conditional

access unit is entitled to view content...entitlements may also include one or more keys...entitlements also may define the time periods for which the conditional access unit may descramble programs" [column 4 lines 50-65].

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
03/29/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436